UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,369	03/30/2004	Douglas S. Ransom	6270/139	4719

46260 7590 04/27/2007

BRINKS HOFER GILSON & LIONE/PML
PO BOX 10395
CHICAGO, IL 60610

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,369	RANSOM ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/04; 05/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 03/30/2004. Claims 1-41 are pending and have been considered as follows.

Examiner's Note

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 41 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Specification

2. The disclosure is objected to because of the following informalities:

- Abstract lines 1 & 2 recites the acronym term "EM" without properly defining it (i.e. "Energy Management (EM)").
- Specification page 3 paragraph 8 line 1 contains improper grammar in the section containing "may coupled." It is noted by the examiner that there appears to be the term "be" missing between the two terms "may" and "coupled."

- Specification page 14 paragraph 71 line 10 recites the acronym term "PKI" without ever defining it. It is noted by the examiner that in view of the specification, the term "PKI" will be interpreted as referring to the public key encryption scheme known commonly at the time of the applicant's invention as "Public Key Infrastructure."

  Appropriate correction is required.

Claim Objections

3. Claim 20 objected to because of the following informalities: The grammar in Claim 20 appears to be improper. The terms "hash" and "encrypt" appear to require the ending "ing" in order to maintain the tense of the claim language so as to read "hashing and encrypting." Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 30 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 30 recites the limitation "said energy distribution network" in Claim 30 line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-4, 14-17, 21, 22, 24-27, & 29-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis (US-6118269-A).

Claim 1:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network comprising,

- "an energy distribution system interface operative to couple said energy management device with at least a portion of said energy distribution system" (i.e. "Information is transmitted between the WAN card 101 and LAN/in-home cards 102 by main bus") [column 4 lines 5-6].
- "a network interface operative to couple said energy management device with said network for transmitting outbound communications to said network, said outbound communications comprising energy management data" (i.e. "a wide area network (WAN) interface card 101, three local area network (LAN) or in-home network interface cards") [column 3 lines 64-66].

- "a processor coupled with said network interface and said energy distribution system interface, operative to generate said energy management data" (i.e. "The microprocessor can receive messages, check CRC and address information, perform TDMA decoding, clocking, bus interface and memory management") [column 5 lines 23-26].
- "a tamper prevention seal coupled with said energy management device, operative to substantially deter unauthorized access to said energy management device and indicate any such access" (i.e. "Tamper-resistant mechanisms may be, for example, padlocks (not shown) provided on meter rings (not shown) used to hold both the enclosure and the meter in place") [column 12 lines 4-7].
- "a seal tamper detection unit coupled with said processor and said tamper prevention seal and operative to detect when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter") [column 12 lines 7-10].

Claim 2:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said tamper seal comprises a revenue seal" (i.e. "According to one embodiment of the utility gateway enclosure according to the present invention, tamper-resistant mechanisms and/or tamper detection mechanisms may be installed with the enclosure") [column 12 lines 1-4].

Claim 3:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said tamper seal comprises a metering point id seal" (i.e. "According to one embodiment of the utility gateway enclosure according to the present invention, tamper-resistant mechanisms and/or tamper detection mechanisms may be installed with the enclosure") [column 12 lines 1-4].

Claim 4:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "a memory coupled with said processor, said memory operative to store confidential data" (i.e. "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM") [column 5 lines 30-31].

Claim 14:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said processor is further operative to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with") [column 12 lines 18-21].

Claim 15:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "a memory coupled with said processor and operative to store at least one device setting and wherein said processor is further operative to prevent changes to said at least one device setting when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM") [column 5 lines 30-31].

Claim 16:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "a memory coupled with said processor and operative to store at least one device setting and wherein said processor is further operative to send a message warning that said device setting has been changed through said network interface when said at least one device setting has been changed after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM") [column 5 lines 30-31].

Claim 17

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "a memory coupled with said processor and operative to store a device configuration, said device configuration having at least one first device setting having a first value, said processor being operative to generate said energy management data based on said first value and to determine that said at least one first device setting has been modified to at least one second value after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, said processor being further operative to generate said energy management data based on said first value and generate alternate energy management data based on said at least one second value in response to said modification" (i.e. "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM") [column 5 lines 30-31].

Claim 21:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said processor is further operative to set off a security alarm when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with") [column 12 lines 18-21].

Claim 22:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "a display coupled with said processor and operative to visually display text, and wherein said processor is further operative to place a warning message on said display when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with") [column 12 lines 18-21].

Claim 24:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said seal tamper detection unit further comprises a sensor operative to detect that said tamper prevention seal is broken" (i.e. "A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter") [column 12 lines 7-10].

Claim 25:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 24 above further comprising,

- "said sensor comprises a limit switch" (i.e. "A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter") [column 12 lines 7-10].

Claim 26:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 24 above further comprising,

- "said sensor comprises a proximity sensor" (i.e. "A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter") [column 12 lines 7-10].

Claim 27:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 26 above further comprising,

- "said proximity sensor comprises at least one of a pin, an optical proximity sensor, an optical motion detector, a grounding tab, an ultrasonic sensor, an electro-magnetic sensor and a gyroscope" (i.e. "A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter") [column 12 lines 7-10].

Claim 29:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "an energy storage device coupled with said seal tamper detection unit and operative to provide power to said seal tamper detection unit in power outage situations" (i.e. "the power supply of the residence or building") [column 11 line 63].

Claim 30:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "said processor is further operative to perform at least one energy management function on said at least a portion of said energy distribution network via said energy distribution system interface" (i.e. "The microprocessor also manages the TDMA transmitter in response to the embedded clock signals in the downstream data packets") [column 5 lines 26-28].
- "said processor further operative to generate said energy management data as a function of said energy management function" (i.e. "The microprocessor also manages the TDMA transmitter in response to the embedded clock signals in the downstream data packets") [column 5 lines 26-28].

Claim 31:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above further comprising,

- "an enclosure defining an interior and an exterior and operative to enclose said energy management device within said interior and to limit access to said energy management device" (i.e. "The first and second chambers 301 and 302 may optionally be accessed by two different panels, thereby allowing for two levels of access, one for the WAN service provider and the other for the LAN service provider") [column 11 lines 48-51].

- "said tamper prevention seal is coupled with said enclosure and operative to substantially deter unauthorized access to said interior of said enclosure and indicate any such access" (i.e. "According to one embodiment of the utility gateway enclosure according to the present invention, tamper-resistant mechanisms and/or tamper detection mechanisms may be installed with the enclosure") [column 12 lines 1-4].

8. Claims 32, 35, 36, 40, & 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Shear et al (US-6157721-A).

Claim 32:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access comprising,

- "generating said data, said data being characterized by an integrity" (i.e. "the load module preferably comprises one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a computer") [column 8 lines 21-28] .
- "detecting when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "the protected processing environment 108 can distinguish between authorized and unauthorized load modules 54 by examining the load module to see whether it bears the seal of verifying authority") [column 9 lines 58-61] .
- "protecting said integrity of said data in response to said detecting" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66] .

Claim 35:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "c) further comprises preventing transmission of said data" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66] .

Claim 36:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "c) further comprises preventing signing of said data" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66] .

Claim 40:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "d) detecting that said at least one first device setting has been modified to have at least one second value" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66] .
- "c) further comprises generating alternate data based on said at least one second value in addition to said data" (i.e. "these specifications 110 are illustrated as a manufacturing tag, but preferably comprises a data file associated with and/or attached to the load module") [column 10 lines 8-11].

Claim 41:

Shear et al discloses a system for protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access comprising,

- "means for generating said data, said data characterized by an integrity" (i.e. "the load module preferably comprises one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a computer") [column 8 lines 21-28] .
- "means for detecting when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "the protected processing environment 108 can distinguish between authorized and unauthorized load modules 54 by examining the load module to see whether it bears the seal of verifying authority") [column 9 lines 58-61].
- "means for taking action to protect said integrity of said data" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66].

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 18 & 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (US-6118269-A).

Claim 18:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above but does not explicitly disclose,

- "said processor is further operative to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Davis does disclose,

- "This increase in voltage may be monitored, for example, by an optocoupler which senses the voltage across the power meter and provides sensor readings to a microprocessor. In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with (i.e., uncoupled from the power meter)" [column 12 lines 18-21].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of sending a notification in the event of an intrusion/tampering.

Claim 28:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 24 above but does not explicitly disclose,

- "said sensor comprises at least one of a camera and a video camera"

However, Davis does disclose,

- "According to one embodiment of the utility gateway enclosure according to the present invention, tamper-resistant mechanisms and/or tamper detection mechanisms may be installed with the enclosure. Tamper-resistant mechanisms may be, for example, padlocks (not shown) provided on meter rings (not shown) used to hold both the enclosure and the meter in place. A tamper detection mechanism may be, e.g., a low-impedance current coil which is connected across the power meter when the gateway is plugged into the power meter" [column 12 lines 7-10].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said sensor comprises at least one of a camera and a video camera," in the invention as disclosed by Davis since cameras and video cameras are forms of devices that may be used as tamper detection mechanisms.

11. Claims 5-13, & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (US-6118269-A) in view of Shear et al (US-6157721-A).

Claim 5:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 4 above but does not disclose,

- "said processor is further operative to delete said confidential data from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to delete said confidential data from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of protecting the processing environment.

Claim 6:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 4 above but does not disclose,

- "said processor is further operative to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of protecting the device environment.

Claim 7:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 4 above but does not disclose,

- "said confidential data comprises a private key operative to sign said energy management data"

However, Shear et al does disclose,

- "Message digest 116 may then be encrypted using asymmetric key cryptography" [column 13 lines 30-31].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a private key operative to sign said energy management data," in the invention as disclosed by Davis for the purposes of encrypting the message digest using public key encryption to ensure the security of data.

Claim 8:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 7 above but does not disclose,

- "said processor is further operative to delete said private key from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to delete said private key from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of ensuring the protection of the device environment by preventing the leak of a private key.

Claim 9:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 7 above but does not explicitly disclose,

- "said processor is further operative to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, and to sign said message with said private key"

However, Davis does disclose,

- "This increase in voltage may be monitored, for example, by an optocoupler which senses the voltage across the power meter and provides sensor readings to a microprocessor. In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with (i.e., uncoupled from the power meter)" [column 12 lines 18-21].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, and to sign said message with said private key," in the invention as disclosed by Davis for the purposes of sending a notification in the event of an intrusion/tampering.

Claim 10:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 4 above but does not disclose,

- "said confidential data comprises a certificate operative to sign said energy management data"

However, Shear et al does disclose,

- "Protected processing environments 108 can use this digital "seal of approval" 106 (which may comprise one or more "digital signatures") to distinguish between authorized and unauthorized load modules" [column 9 lines 52-55].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a certificate operative to sign said energy management data," in the invention as disclosed by Davis for the purposes of authorization.

Claim 11:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 10 above but does not disclose,

- "said processor is further operative to delete said certificate from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to delete said certificate from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of protecting the device environment.

Claim 12:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above but does not disclose,

- "said processor is further operative to prevent said transmitting of said energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to prevent said transmitting of said energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of protecting the device environment.

Claim 13:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above but does not disclose,

- "said processor is further operative to prevent said transmitting of signed energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to prevent said transmitting of signed energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of protecting the device environment.

Claim 23:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above but does not disclose,

- "said processor is further operative to mark said energy management data as unreliable when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Shear et al does disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal" [column 9 lines 64-66].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to mark said energy management data as unreliable when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of determining which data is non-authorized and discarding them in order to protect the device environment.

12. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (US-6118269-A) in view of Schneier et al (US-5978475-A).

Claim 19:

Davis discloses an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 1 above but does not disclose,

- "said processor is further operative to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"

However, Schneier et al does disclose,

- "Audit logs have long been used to keep permanent records of critical events. The basic idea is that the audit log can be used at some future date to reconstruct events that happened in the past. This reconstruction might be required for legal purposes (to determine who did what when), for accounting purposes, or to reconstruct things after a disaster: errors, loss of data, deliberate sabotage, etc" [column 1 lines 1-10].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Davis for the purposes of keeping track of events to be used in various venues (i.e. forensics, error debugging, data/system recovery, etc).

13. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (US-6118269-A) in view of Schneier et al (US-5978475-A) in further view of Shear et al (US-6157721-A).

Claim 20:

Davis and Schneier et al disclose an energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network as in Claim 19 above but do not disclose,

- "said processor is further operative to at least one of hash and encrypt said audit log"

However, Shear et al does disclose,

- "In the FIG. 5 process, load module 54 (along with specifications 110 if desired) is processed to yield a "message digest" 116 using a conventional one-way hash function selected to provide an appropriate resistance to algorithmic attack" [column 13 lines 4-8].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said processor is further operative to at least one of hash and encrypt said audit log," in the invention as disclosed by Davis for the purposes of additional security against tampering especially since audit log files are the only source of information disclosing events.

14. Claims 33, 34, & 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shear et al (US-6157721-A) in view of Davis (US-6118269-A).

Claim 33:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "c) further comprises deleting said confidential data" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66].

but Shear et al does not disclose,

- "said energy management device stores confidential data"

However, Davis does disclose,

- "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM" [column 5 lines 30-31].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said energy management device stores confidential data," in the invention as disclosed by Shear et al for the purposes of storage.

Claim 34:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "c) further comprises preventing access to said confidential data" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66].

but Shear et al does not disclose,

- "said energy management device stores confidential data"

However, Davis does disclose,

- "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM" [column 5 lines 30-31].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said energy management device stores confidential data," in the invention as disclosed by Shear et al for the purposes of storage.

Claim 37:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 but does not disclose,

- "c) further comprises generating a warning message"

However, Davis does disclose,

- "This increase in voltage may be monitored, for example, by an optocoupler which senses the voltage across the power meter and provides sensor readings to a microprocessor. In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with (i.e., uncoupled from the power meter)" [column 12 lines 18-21].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises generating a warning message," in the invention as disclosed by Shear et al for the purposes of notifying that an intrusion/tampering has occurred.

Claim 38:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above further comprising,

- "c) further comprises preventing changes to said device settings" (i.e. "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal") [column 9 lines 64-66].

but Shear et al does not disclose,

- "said energy management device stores device settings"

However, Davis does disclose,

- "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM" [column 5 lines 30-31].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said energy management device stores device settings," in the invention as disclosed by Shear et al for the purposes of storage.

Claim 39:

Shear et al discloses a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access as in Claim 32 above but does not disclose,

- "said energy management device stores device settings"
- "c) further comprises generating a warning message if said device settings are changed"

However, Davis does disclose,

- "The microprocessor may be an 80C51XA made by Philips Electronics or in the Motorola 68000 family with internal ROM, RAM and EEROM" [column 5 lines 30-31].
- "This increase in voltage may be monitored, for example, by an optocoupler which senses the voltage across the power meter and provides sensor readings to a microprocessor. In turn, the microprocessor initiates communication with a headend or other monitoring station to indicate that the gateway has been tampered with (i.e., uncoupled from the power meter)" [column 12 lines 18-21].

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "said energy management device stores device settings," and "c) further comprises generating a warning message if said device settings are changed," in the invention as disclosed by Shear et al for the purposes of storage and notifying that an intrusion/tampering has occurred.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Smith (US-6233685-B1) – tamper resistance

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
04/17/2007

James Myhre
Supervisory Patent Examiner